PENGAMANAN ARSIP ELEKTRONIK MENGGUNAKAN *PUBLIC KEY INFRASTRUCTURE*

Supapri Situmorang[1], Ardya Suryadinata[2], Yopie Maulana S.[3]
[1,2,3]*Sekolah Tinggi Sandi Negara, Jalan Haji Usa, Ciseeng, Bogor 16330*
Email : supapri@yahoo.com[1], ardyasuryadinata@yahoo.com[2], yopie.maulana@gmail.com[3]

ABSTRAK

Perkembangan teknologi informasi yang sangat pesat telah mengubah paradigma kehidupan manusia, termasuk di dalamnya perkembangan terhadap arsip, yang pada awalnya disimpan dalam bentuk fisik di dalam lemari arsip menjadi file-file yang diarsipkan dalam bentuk arsip elektronik yang disimpan dalam database.Perkembangan ini tentunya menimbulkan sebuah permasalahan baru terkait pengamanan arsip yang disimpan dalam bentuk elektronik. Pengamanan arsip elektronik tidak hanya mencakup pengamanan secara fisik terhadap media penyimpanan, tetapi juga pengamanan terhadap arsip elektronik tersebut, terutama terhadap ancaman berupa pencurian, pengrusakan, dan pengubahan arsip elektronik. Pada makalah ini, kami akan mengajukan salah satu solusi terhadap pengamanan arsip elektronik secara kriptografi dengan menggunakan Public Key Infrastructure (PKI) sehingga integritas, ketersediaan, kerahasiaan, dan anti-penyangkalan terhadap arsip elektronik itu sendiri dapat terjamin. Dalam makalah ini pertama-tama kami akan menjelaskan mengenai arsip elektronik beserta aspek-aspek keamanan yang perlu diperhatikan dan selanjutnya kami akan menjelaskan mengenai PKI dan pengunaannya dalam pengamanan arsip elektronik.

Kata kunci*:* Public key infrastructure, PKI, Arsip, Arsip elektronik

1. PENDAHULUAN

Perkembangan teknologi yang sangat cepat telah mengubah paradigma kehidupan masyarakat. Dahulu, masyarakat lebih cenderung menggunakan sistem yang manual. Akan tetapi, seiring dengan perkembangan teknologi dan informasi, secara perlahan namun pasti paradigma tersebut mulai bergeser. Masyarakat mulai memasuki era baru, yaitu era digital. Dewasa ini digitalisasi telah mengubah berbagai segi kehidupan masyarakat, termasuk salah satunya dalam dalam cara pengarsipan.

Sebelum era digital, proses pengarsipan dilakukan secara manual, misalnya dengan menyimpan dokumen-dokumen dalam sebuah map yang kemudian disimpan di dalam lemari arsip. Tentunya cara seperti ini tidak efektif dan efisien karena semakin banyak dokumen yang akan diarsipkan maka akan semakin besar juga ruang yang dibutuhkan untuk menyimpan arsip tersebut. Selain itu, proses pencarian terhadap arsip tertentu juga akan mempunyai kendala tersendiri karena pencarian terhadapa arsip harus dilakukan secara manual dengan menyisir arsip satu per satu. Dari segi kemanan, arsip yang disimpan dalam bentuk fisik, seperti dokumen yang disimpan di dalam map, lebih rentan terhadap pencurian, pamalsuan, dan kerusakan.

Sekarang ini, pengarsipan dilakukan secara elektronik dengan dokumen-dokumen yang disimpan dalam bentuk file-file elektronik. Dengan cara ini, pengarsipan dapat dilakukan dengan lebih efisien dan efektif karena proses pencarian lebih cepat dan tidak membutuhkan ruang penyimpanan yang besar. Naamun demikian, di samping berbagai kelebihan yang diberikan oleh perngarsipan secara elektronik, timbul permasalahan baru berkaitan dengan pengamanan arsip elektronik. Arsip elektronik rawan terhadap ancaman yang berupa pencurian, pengrusakan, atau pengubahan arsip. Untuk menghadapi berbagai ancaman tersebut, dibutuhkan suatu teknik yang dapat menjamin kerahasiaan, keaslian, dan keutuhan dari data yang disimpan dalam bentuk arsip elektronik. Salah satu teknik yang dapat kita gunakan adalah dengan menggunakan *Public Key Infrastructure* (PKI).

Dalam makalah ini, pertama-tama penulis akan membahas konsep dari arsip elektronik dan PKI beserta dengan komponen-komponen yang terlibat di dalamnya. Pada bagian selanjutnya akan dijelaskan mengenai bagaimana pengamanan arsip elektronik dengan menggunakan PKI beserta dengan aspek keamanan yang diberikan.

2. LANDASAN TEORI

Arsip

Menurut UU Nomor 7 Tahun 1971 yang dimaksud dengan arsip adalah Naskah-naskah yang dibuat dan diterima oleh Lembaga-Lembaga Negara, Badan-Badan Pemerintahan atau Swasta, dan atau perorangan dalam bentuk corak apapun, baik dalam keadaan tunggal maupun berkelompok, dalam rangka pelaksanaan kegiatan pemerintahan dan kehidupan kebangsaan.

Sesuai dengan pengertian di atas, arsip adalah informasi dari suatu aktifitas atau kejadian yang tersimpan dalam suatu media (kertas, video, kaset, media elektronik) yang berlangsung di dalam suatu lembaga, instansi atau perorangan, baik dalam keadaan tunggal maupun jamak.

Berdasarkan media penyimpanannya, arsip dapat dibedakan menjadi:

1. Arsip berbasis kertas. Arsip yang berupa teks atau gambar atau numerik yang tertuang di atas kertas.
2. Arsip pandang-dengar(audio-visual). Merupakan arsip yang dapat dilihat dan didengar, contohnya seperti kaset, atau pita video.
3. Arsip kartografik dan arsitektural. Arsip berbasis kertas tetapi isinya memuat gambar grafik, peta, maket, atau gambar arsitek lainnya, dan karena bentuknya unik dan khas maka dibedakan dari arsip berbasis kertas pada umumnya.
4. Arsip elektronik merupakan arsip yang dihasilkan oleh teknologi informasi, khususnya komputer

Sedangkan, berdasarkan fungsinya, arsip dibedakan menjadi:

1. Arsip dinamis
   a. Arsip dinamis aktif yaitu arsip yang masing-masing digunakan secara langsung dalam penyelesaian suatu kegiatan. Dengan demikian arsip aktif ini juga merupakan berkas kerja.
   b. Arsip dinamis inaktif yaitu arsip yang sudah tidak digunakan secara langsung dalam penyelesaian kegiatan, karena kegiatan sudah selesai tetapi sewaktu-waktu masih diperlukan sehingga perlu disimpan.
2. Arsip statis yaitu arsip yang sudah tidak lagi digunakan dalam kegiatan oleh penciptanya, tatapi mempunyai nilai tertentu sehingga pantas untuk dilestarikan untuk kepentingan umum, sejarah, atau sebagai bahan bukti dan pertanggungjawaban nasional.

Proses terjadinya arsip umumnya melalui beberapa tahap sebagai berikut:

1. Tahap penciptaan dan penerimaan
   Arsip dinamis dimulai dari penciptaan atau penerimaan dokumen.
2. Tahap distribusi
   Penyebaran arsip kepada semua pihak yang berkepentingan.
3. Tahap penggunaan
   Penggunakan untuk kepentingan tertentu sesuai maksud dan tujuan penciptaannya arsip.
4. Tahap pemeliharaan
   Arsip aktif yang sudah mengalami penurunan fungsinya menjadi inaktif tetapi harus dipelihara karena menjadi sumber informasi, sumber data, dan sebagai bahan bukti pertanggungjawaban. Pada tahap ini arsip dinamis diberkaskan menurut urutan atau susunan yang telah ditentukan sebelumnya. Kegiatan retrieval atau penemuan kembali mengacu kepada penemuan informasi yang terdapat pada berkas yang diminta.
5. Tahap pemusnahan
   Arsip dinamis inaktif yang sudah habis masa simpan dan tidak mempunyai nilai khusus yang dianggap permanen dapat dimusnahkan.

2.1 Kriptografi Kunci Publik

Kriptografi kunci publik adalah sistem kriptografi yang menggunakan kunci yang berbeda untuk enkripsi dan dekripsi. Berarti ada 2 kunci di sini, yang disebut kunci publik untuk kunci enkripsi dan kunci privat untuk kunci dekripsi [2]. Pada kriptografi kunci publik, kunci yang digunakan untuk mengenkripsi dapat

disebarkan secara umum kepada pihak-pihak lain yang perlu berkomunikasi, sedangkan kunci privat harus dijaga kerahasiaannya oleh pihak yang memilikinya. Salah satu keuntungan yang diberikan dari sistem ini adalah pendistribusian dari kunci yang digunakan untuk berkomunikasi menjadi lebih mudah jika dibandingkan dengan sistem kriptografi simetris yang hanya menggunakan satu kunci baik untuk enkripsi maupun dekripsi pesan.

2.2 Public Key Infrastructure

Public Key Infrastructure yang selanjutnya akan disingkat PKI adalah Infrastruktur sekuriti yang diimplementasikan menggunakan konsep dan teknik kriptografi kunci publik [1]. PKI merupakan infrastruktur keamanan yang memungkinkan pengguna secara aman dan rahasia saling bertukar datapada jaringan publik seperti internet dengan menggunakan pasangan kunci publik dan privat yang didapatkan dan didistribusikan melalui pihak ketiga yang terpercaya. PKI menyediakan sertifikat digital (*digital certificate*) dan layanan direktori yang dapat menyimpan sertifikat digital dan jika diperlukan melakukan revokasi/pencabutan sertifikatnya. Dengan kata lain PKI merupakan infrastruktur dasar yang dapat digunakan untuk mendukung penggunaan *public key* kriptografi secara aman, pada salah satunya yaitu transaksi elektronik melalui internet.

Pada umumnya arsitektur dasar dari PKI memiliki beberapa komponen antara lain:

1. *Certification Authority* (CA)

   Certification Authority (CA) adalah sebuah lembaga/institusi atau perorangan yang bertugas mengeluarkan sertifikat, yang mengesahkan pasangan kunci publik dengan identitas pemilik kunci tersebut atau dengan kata lain mensertifikasi jati diri *subscriber*/*subject* agar *subscriber* itu bisa dikenali di dunia digital, dengan menerbitkan sertifikat digital untuk tiap *subscriber*nya.

2. Kebijakan Keamanan (Security Policy)

   Kebijakan keamanan biasanya berupa dokumen yang bersifat legal, berisi langkah-langkah kebijakan organisasi dalam pengamanan informasi, serta proses dan teknik kriptografi yang digunakan.

3. *Registration Authority* (RA)

   Registration authority (RA) bertanggung jawab untuk melakukan proses identifikasi dan otentikasi terhadap subscriber dari sertifikat digital, tetapi tidak menandatangani sertifikat itu.
   Adanya sebuah RA dalam PKI memang sifatnya optional (tidak harus ada), karena memang RA hanya menjalankan beberapa tugas yang didelegasikan oleh CA jika CA tidak sanggup melakukannya. Artinya, bisa saja dalam suatu skenario tertentu, seluruh tugas RA berada dalam CA. Menurut Adams dan Lloyd, tugas-tugas RA dapat mencakup:

   - Otentikasi calon subscriber secara fisik
   - Registrasi calon subscriber
   - Membuat pasangan key untuk subscriber (jika subscriber tidak sanggup membuat sendiri pasangan kuncinya).
   - Membuat backup dari kunci privat yang dipergunakan untuk enkripsi (*key recovery*)
   - Pelaporan kalau ada sertifikat yang dicabut (*revocation reporting*)

4. *Certificate Repository*

   Certificate Repository adalah suatu database yang bertanggung jawab untuk menyimpan dan menjamin ketersediaan sertifikat dan Certificate Revocation List (CRL) agar dapat diakses secara luas oleh pengguna PKI. CRL disini merupakan suatu daftar yang digunakan untuk mengecek status atau validitas dari suatu sertifikat.

5. Subject atau subscriber

   Subscriber dari sebuah sertifikat digital tidaklah harus orang atau perusahaan, namun bisa juga peralatan (device) pada jaringan, aplikasi software dan downloadable application. Seorang subscriber harus bisa menjaga private key-dengan baik, jangan sampai tercuri oleh orang lain.

2.3 Tanda Tangan Digital

Tanda tangan digital digunakan untuk mengecek otentikasi dari pihak yang membuat suatu dokumen. Proses penanda tanganan digital suatu dokumen dilakukan dengan menggunakan kunci privat dari pihak yang membuat dokumen tersebut. Oleh karena kunci privat hanya diketahui oleh pihak yang memilikinya, maka keaslian bahwa suatu dokumen memang benar dibuat oleh pihak yang menandatanganinya dapat terjamin. Untuk dapat mengecek tanda tangan digital pada suatu dokumen digunakan kunci publik dari pihak yang menandatangani dokumen tersebut.

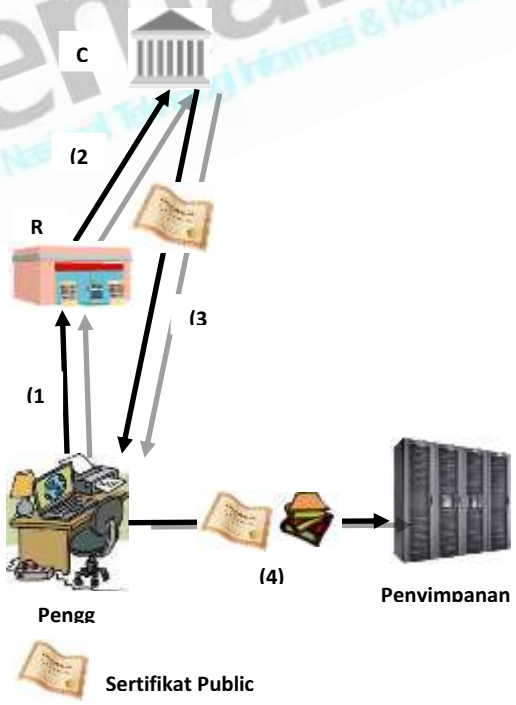
2.4 Sertifikat Kunci Publik

Public key certificate adalah suatu sarana yang memungkinkan *public key* dapat disimpan, didistribusikan atau diteruskan melalui *unsecured media* tanpa bahaya manipulasi yang tidak terdeteksi. Sasaran metode ini adalah untuk membuat *public key* dari entitas tertentu tersedia untuk entitas lain yang keaslian dan kebenarannya teruji [2].

Sebuah sertifikat public key berisi bagian data dan bagian tanda tangan. Bagian data berisi nama dari pihak yang memiliki public key, public key yang berdangkutan , dan informasi tambahan lainnya. Sedangkan bagian tanda tangan berisi tanda tangan dari CA yang mengeluarkan sertifikat tersebut. Untuk pihak lain yang akan memverifikasi suatu sertifikat, pihak tersebut harus memiliki salinan public key CA yang mengeluarkan sertifikat tersebut. Selanjutnya pihak tersebut harus memverifikasi tanda tangan yang tertera di dalam sertifikat dengan menggunakan public key CA. Apabila hasil verifikasi benar, maka sertifikat tersebut asli dan dapat digunakan untuk berkomunikasi.

3. PENGAMANAN ARSIP DENGAN PKI

Seperti yang telah dijelaskan sebelumnya, terdapat beberapa tahap terjadinya suatu arsip, yaitu tahap penciptaan dan penerimaan, tahap distribusi, tahap penggunaan, tahap pemeliharaan, dan tahap pemusnahan arsip. Di dalam makalah ini penulis akan lebih berfokus pada pengamanan arsip pada tahap pemeliharaan dan pemusnahan.



Gambar 1 Skema Pengamanan Arsip Digital

Pada skema di atas, pengguna yang dalam hal ini dapat berupa individu atau suatu bagian dari organisasi pertama-tama akan membuat sertifikat digital dengan cara mendaftarkan publik key yang ia miliki beserta identitas lain yang dibutuhkan kepada RA. Kemudian RA akan mengecek keabsahan dari identitas yang diberikan dan apabila tidak terdapat masalah maka selanjutnya RA akan memberikan public key dan identitas pengguna kepada CA untuk dibuat sertifikat dan selanjutnya ditandatangani oleh CA.
Sertifikat yang telah ditandatangani oleh CA kemudian akan dikembalikan kepada pengguna yang bersangkutan. Pengguna tersebut selanjutnya dapat menyebarkan sertifikat yang ia miliki kepada pihak-pihak lain yang perlu berkomunikasi dengannya, termasuk juga kepada pihak penyimpan arsip.

Selanjutnya, apabila pengguna ingin menyimpan arsip dokumen kepada penyimpanan arsip, pengguna tersebut pertama-tama harus menandatangani arsip dokumen tersebut dengan kunci privat yang ia miliki dan selanjutnya mengirimkan arsip dokumen tersebut kepada penyimpanan arsip. Pihak penyimpanan arsip yang menerima arsip dokumen tersebut selanjutnya akan mengecek keabsahan dari tanda tangan digital yang tertera pada arsip dokumen dengan menggunakan public key pengguna yang ia peroleh dari setifikat digital. Apabila semuanya benar dan sah, pihak penyimpan arsip selanjutnya akan menyimpan arsip tersebut dengan teknik pengamanan yang diatur dalam kebijakan keamanan organisasi yang bersangkutan.

Apabila sewaktu-waktu arsip yang telah disimpan tersebut dibutuhkan oleh pengguna yang memilikinya atau pengguna lain yang membutuhkannya, maka pengguna tersebut harus terlebih dahulu mengirimkan pengajuan permintaan yang telah ditandatangani oleh pemilik arsip yang sah. Hal ini bertujuan agar pengguna yang mengajukan benar-benar telah memperoleh izin dari pemilik arsip yang sah. Selanjutnya, pihak penyimpan arsip akan mengecek keabsahan dari tanda tangan yang terdapat pada pengajuan permintaan tersebut. Apabila tanda tangan tersebut sah, maka pihak penyimpan arsip selanjutnya akan mengirimkan arsip yang diminta beserta dengan tanda tangan digital dari pihak penyimpan arsip. Pihak pengguna yang telah menerima arsip tersebut selanjutnya akan memeriksa keabsahan dari tanda tangan pihak penyimpan arsip untuk memastikan keaslian dari arsip yang dikirimkan.

5. KESIMPULAN

Berdasarkan pembahasan di atas, maka penulis mengambil kesimpulan bahwa penggunaan PKI dalam pengamanan arsip digital dapat memberikan kemudahan dalam penyimpanan dan pengambilan arsip oleh pihak-pihak yang berhak dengan tetap menjamin keaslian dan keutuhan dari arsip tersebut.

DAFTAR PUSTAKA

[1] C. Adams, and S. Lloyd, *Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations,* (Indianapolis, Macmillan Technical Publishing: 2000).
[2] Sumarkidjo, dkk, *Jelajah Kriptologi, LEMSANEG, Jakarta:2007*
[3] Menezes, A.J., van Oorsschoot, P.C., Vansto e, S.A.; *Handbook of Applied Cryptography*, CRC Press, 1996.
[4] Schneier, B.; *Applied Cryptography*, 2nd ed., John Wiley &Sons, Inc., 1996.
[5] Sutrisno,*Administrasi Perkantoran Modern, Prajabatan Golongan II,* Jakarta:Lembaga Administrasi Negara:2009
[6] UU Nomor 7 Tahun 1971 tentang Ketentuan-Ketentuan Pokok Kearsipan